Exploiting Channel Fragmentation and Aggregation/ Bonding to Create Security Vulnerabilities

S. Anand, S. Sengupta, K. Hong, K. P. Subbalakshmi, R. Chandramouli and Hasan Cam

***Abstract*—We address a unique security vulnerability due to spectrum fragmentation, aggregation and bonding in OFDMA based wireless networks. Specifically, we address security threats in IEEE 802.22 based dynamic spectrum access (DSA) networks and in LTE and HSPA+ networks. Typically, channel fragmentation, aggregation/bonding have been perceived as a means to enhance the bandwidth and throughput for the users. However, this could also result in the loss of orthogonality between the bonded or fragmented spectrum bands. We show that this leads to a security vulnerability that can be exploited by an attacker to cause service disruption. In this case, the attacker need not even operate in the same bands as the user, to be effective. The security vulnerability discussed here is shown to result in various amounts of service disruption based on the strategy of attackers, the radio network parameters and the user locations.**

We present an analysis of two types of attacks- the MAXIMP attack according to which the attacker (which could indicate an individual attacker or a set of colluding attackers) tries to cause maximum service disruption by transmitting at as large power as possible and the MINPOW attack, where in, the attacker transmits at minimum power to just create a targeted level of service disruption. Results indicate that MAXIMP attack can cause up to about 16% loss in the capacity of the system. Results also indicate that the system is susceptible to about 11-15% loss in throughput when the malicious attacker launches the MINPOW attack.

We finally study means to detect the attack. We present an individualistic detection mechanism of the attack, where in each individual node uses a received energy based detection. We also provide a mechanism by which, nodes can co-operate in a centralized manner to improve the process of detecting the attack. Results indicate that the MINPOW attack is more difficult to detect than the MAXIMP attack. However, the detection can be improved by centralized co-operation. *To the best of our knowledge, this is the first attempt to identify, analyze and detect a security vulnerability due to channel fragmentation, aggregation and bonding.*

Index Terms – Channel fragmentation, aggregation/bonding, vulnerability, service disruption.

This paper was presented in part in IEEE ICC 2011 [1] and in part, in IEEE GLOBECOM 2011 [2]. In addition to the analysis presented in [1] and [2], we also add mechanisms to detect the attack in an individualistic manner as well as by centralized co-operation.

S. Anand is with the Department of Technology Management and Innovation, Polytechnic Institute of New York University. E-mail: as8547@nyu.edu

S. Sengupta is with the Department of Computer Science and Engineering, University of Nevada, Reno. E-mail: ssengupta@unr.edu

K. Hong, K. P. Subbalakshmi and R. Chandramouli are with the Department of ECE, Stevens Institute of Technology. E-mail: {khong,ksubbala,mouli}@stevens.edu

Hasan Cam is with the United States Army Research Labs. E-mail: hasan.cam.civ@mail.mil

I. Introduction

Dynamic spectrum access (DSA) [3] based cognitive radio networks [4] were developed as a solution to the under utilization of spectrum due to fixed spectrum allocation. Unlicensed "secondary" users use the spectrum (called white spaces) unused by the licensed "primary" users. The IEEE 802.22 wireless regional area networks (WRAN) [5] emerged as the first standards for cognitive radios. The physical layer (PHY) and medium access control (MAC) specifications for secondary to use the white spaces in the television (TV) transmission band can be found in [6]. The IEEE 802.22 standard specify policies for channel fragmentation, bonding and aggregation. Similarly, next generation wireless networks like the advanced long term evolution (LTE) and high speed packet access (HSPA+) also define carrier aggregation and bonding to increase the bandwidth and throughput for users. Carrier bonding refers to combining contiguous spectrum bands (e.g., two bands of 20 MHz each) to provide a user, larger (e.g., 40 MHz) bandwidth. Alternatively, non-contiguous spectrum bands can be aggregated (called as carrier aggregation) [7], [8] and allocated to users. Channel fragmentation refers to allocating a portion of a spectrum band , e.g., if a channel has a bandwidth of 6 MHz, fragmentation allows allocation of a portion of the spectrum band corresponding to a bandwidth of 2 MHz to a user. We identify a potential security vulnerability resulting due to these three features. We illustrate the practicality of the attack by test-bed experiments followed by a detailed theoretical analysis.

Channel fragmentation, aggregation and bonding were studied as a means to enhance the spectrum utilization in DSA networks [9]-[13] and the references therein, as well as 802.11n wireless LANs [14]. Recently, T-Mobile announced that they would bond two contiguous 5MHz channels in HSPA+ [15], that yield 21 Mbps each, to achieve a theoretical throughput of 42 Mbps. Verizon Wireless and AT&T Wireless then proposed channel aggregation [7], [8] (of non-contiguous channels, aggregating the 700 MHz and 3.6 GHz bands) for LTE networks and by using Qualcomm's Mediaflo spectrum [16], which can theoretically result in double the data rate for LTE users. The RAN working group of the third generation partnership project (3GPP) provide the technical specifications for carrier aggregation and bonding in order to provide higher bandwidths and throughputs for the long term evolution (LTE) [17] and high speed packet access (HSPA+) [18] users. Sengupta *et al* [9] proposed a utility based graph coloring algorithm that presented the advantages using channel fragmentation and aggregation. In [10], Song and Lin present and enhanced MAC

protocol for DSA networks, where the effectiveness of channel fragmentation, aggregation and bonding were demonstrated by achieving enhanced throughput. Bahl *et al* provided an experimental set up for channel assignment that utilizes the white spaces in the spectrum. An architecture for the utilization of DTV white spaces incorporating channel fragmentation was provided in [12]. A detailed study of channel fragmentation and related works can be found in [13].

Although channel fragmentation, aggregation and bonding resulted in larger throughput, we identify an important security vulnerability resulting due to these features. Typically the IEEE 802.22, 802.11n, LTE and HSPA+ networks use orthogonal channels for transmission. Fragmentation, aggregation or bonding of channels can result in loss of orthogonality and hence, mutual interference or "leakage" from one channel to the other. The 3GPP LTE standards and the IEEE 802.22 standards do specify means to maintain orthogonality after channel fragmentation, aggregation and bonding but this can still result in leakage into other neighboring spectrum bands thus causing service disruption like the one discussed in this paper. As an example, the super G product [19] demonstrated how channel aggregation of channel 1 and 11 in the 802.11g system can adversely affect channel 6. In [20], Deek *et al* showed by experiments that while performing channel bonding, a user transmitting a small power on an adjacent channel can result in significant degradation of the throughput due to leakage. Similar effects were observed in IEEE 802.11a WiFi systems due to adjacent channel interference [21]. The authors showed that transmission by low data rate users can affect high data rate users adversely causing more than 80% degradation in the average throughput. While adaptive guard bands (e.g., Yang et al [22]) demonstrated some resilience to the leakage effects, the implementation was found to be extremely complex.

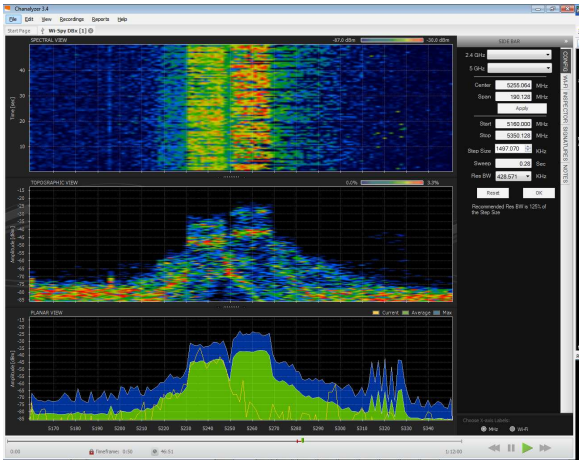


Fig. 1. Test-bed experiment demonstrating leakage on other channels due to bonding.

To illustrate the service disruption, we conduct test bed experiments by implementing a cognitive radio prototype [23] on a software abstraction layer over off-the-shelf IEEE 802.11 a/b/g supported by Atheros hardware chip sets. We bond two channels (corresponding to 5.24 GHz and 5.26 GHz) and measure the power on all the other channels. Fig. 1 provides the wispy image of our experimental results. The green color in the bottom-most picture in the wispy image in Fig. 1 represents the average power on the channels and the blue color represents the peak powers measured on the channels. The channel with the highest peak power is the one on which transmission takes place. It is observed that a significant power on the bonded channel (more than -40 dBm) results in a significant leakage on the neighboring spectrum bands. Note that, the value of -40dBm is just one of the examples we used in this experiment scenario. Any high power used on the bonded channel created adverse effect on the neighboring channels. This is a consequence of the loss of orthogonality between spectrum bands resulting due to bonding. Similar consequences can also be expected for channel fragmentation and aggregation.

The leakage demonstrated in Fig. 1 can result in a unique denial of service (DoS) in wireless networks. A set of colluding malicious attackers can exploit the correlation between the non-orthogonal fragments (resulting due to fragmentation or aggregation or bonding) and cause service disruption. Service disruption in wireless networks have traditionally been viewed as jamming attacks [24]. Cognitive radios are also susceptible to multi-channel jamming [25] where the jammer can switch channels to jam multiple channels or the attacker chooses a particular set of channels and jam them [26]. However, the service disruption threat due to fragmentation, aggregation/bonding is significantly different because the malicious attackers can now transmit on channel j to cause service disruption on channel i. The attack exploits the loss of orthogonality between channels which is a consequence of fragmentation, aggregation and bonding. The service disruption need not be a complete DoS, but can be a loss in the channel capacity or loss in throughput, thus resulting in degraded quality-of-service (QoS). This issue may be more prominent in channel bonding, because channel aggregation does not result in loss of orthogonality [17]. However, channel aggregation can result in leakage into other neighboring spectrum bands. As an example, consider the aggregation of the 1.8 GHz, 2.1 GHz and 2.6 GHz bands in LTE [27]. This results in a high correlation (about 0.4) with the 2.4 GHz WiFi spectrum band and can cause leakage into the WiFi band.

In this paper, we present a detailed analysis of service disruption attacks due to carrier fragmentation, aggregation and bonding. We specifically consider two kinds of attacks. The first is a *system level attack* called the MAXIMP attack [1], where in, the colluding malicious attackers aim to create maximum leakage for *all* the users in the system, by transmitting at as large a power as possible. This is typically expected in IEEE 802.22 based DSA networks. Here, secondary users can enter and leave a network dynamically. Therefore, the multiple malicious cannot target any specific user, bu can only launch a system-wide attack by colluding to operate on the same spectrum fragment at as high a power as they can.

In cellular networks like the advanced LTE and HSPA+ networks, it is practically infeasible for malicious users to transmit at large powers. Moreover, in such systems, users enter the network with a specific user identifier like the international mobile subscriber identity (IMSI) [17], [18] and allow

attackers to target specific users to launch their attacks. Here, a set of malicious attackers wish to create sufficient disruption in service to certain users by transmitting at minimum power. This kind of attack, called the MINPOW attack [2], is also discussed in this paper .

We also discuss mechanisms to detect the attack. We use the received power at a user and develop a hypothesis test to determine if the service disruption was due to leakage because of transmission by good users or whether the service disruption was due to an attack launched by the malicious attackers. We first develop an individual detection mechanism and then improve the detection by centralized co-operation between the users.

Numerical results indicate that at low transmit powers (i.e., for low number of colluding malicious attackers) malicious attackers do not cause significant loss in the capacity by launching the MAXIMP attack. However, for larger transmit powers (i.e., large number of colluding malicious attackers), the MAXIMP attack can result in service disruption causing upto about 16% loss in the channel capacity. In terms of data rates, this could be between 200 Kbps to 9 Mbps. Results also indicate that the MINPOW attack can cause about 70% loss of throughput in LTE networks and about 11-15% in HSPA+ networks. The physical interpretation is that aggregating two channels of 20 MHz, 20 Mbps, each, to yield a 40 MHz spectrum band will not provide a throughput of 40 Mbps, but instead can yield about 11-15% less, i.e., about 34 Mbps throughput, which is a significant loss in throughput of about 6 Mbps. In other words, the total bandwidth obtained by aggregation or bonding of carriers is less than the sum of its parts. Also, numerical results show that users farther from the base station suffer higher throughput degradation due to the MINPOW attack in LTE networks, while the attack causes higher degradation in throughput for near users in HSPA+ networks. Finally, it is observed that MAXIMP attacks can be detected more easily than MINPOW attacks. Also, MINPOW attacks are more likely to be detected in the LTE network than in the HSPA network. *To the best of our knowledge, this is the first attempt to identify and analyze a significant security vulnerability due to carrier fragmentation, aggregation and bonding in IEEE 802.22, Advanced LTE and HSPA+ networks. Note that the attacks we discuss in this paper is fundamentally different from leakage in non-orthogonal FDMA systems. While leakage in non-orthogonal FDMA systems is an uncontrolled and unintentional phenomenon, the attacks discussed here are systematically launched by colluding malicious nodes with a specific intention to cause service disruption.*

The rest of the paper is organized as follows. Sections II and III discuss the MAXIMP and MINPOW attacks, respectively. Section IV presents the mechanisms to detect the attacks. Numerical results are provided in Section V and conclusions are drawn in Section VI.

II. MAXIMP Attack

Consider a DSA network (e.g, an IEEE 802.22 WRAN) with N orthogonal channels which can be used by secondary users when the primary users are inactive. Each of these N channels can be fragmented into K sub-channels. Henceforth, throughout this section, "channel" refers to one of the NK fragments in the system, unless explicitly mentioned otherwise. The NK fragments need not be mutually orthogonal, in general. Therefore, when signals are transmitted in the i^{th} fragment $(1 \leq i \leq NK)$, it causes energy leakage in the j^{th} fragment $(j \neq i)$. This kind of energy leakage can be exploited by colluding malicious nodes in the network to disrupt the communication of the other good secondary users in the system.

Since users can dynamically enter and leave a network, it is very complex for attackers to target a specific user in this case. Then, the attackers launch a system-wide attack. The set of malicious attackers each transmit signals on different channels in such a way that causes significant interference and hence, service disruption to legitimate users on all the channels. To launch the MAXIMP attack, it is of interest to determine the MAXimum IMPact (or service disruption) that can be caused by a set of malicious attackers to the good secondary users in the system. In order to perform the analysis, we consider the following system.

- There are NK fragments such that the correlation between fragments i and j is ρ_{ij}. If the corresponding fragments are orthogonal, then $\rho_{ij} = 0$. In general, ρ_{ij} represents the co-variance between fragments i and j.
- The attacker transmitting on channel i, transmits a signal with signal strength, E_i, that corresponds to a power, $P_i = |E_i|^2$.
- The total power that can be transmitted by the attackers on all the channels is P_{tot}. This constraint is incorporated to account for the maximum transmit power of the malicious nodes as well as the fact that P_{rmtot} is lesser in magnitude than the transmit power that actually results in jamming of the channels.

Let $\mathbf{C} = [c_{ij}]_{\substack{1\leq i\leq NK \\ 1\leq j\leq NK}}$, where $c_{ij} = \rho_{ij}$, $\forall\ i \neq j$ and $c_{ii} = 0$, $\forall\ i$, represent the co-variance between channels i, j, $\forall\ i \neq j$. Let Let $\mathbf{e} = [E_i]_{1\leq i\leq NK}$ represent the vector of field strengths on all the channels (each malicious node transmits on a different channel) and let $\mathbf{p} = [P_i]_{1\leq i\leq NK}$ be the vector of corresponding powers. Signals transmitted on any channel cause a leakage on the other channels since the fragmented channels are not orthogonal in general. The leakage caused by the attackers on the i^{th} channel, l_i, can be written as

$$l_i = \textstyle\sum_{j=1}^{NK} c_{ij} E_j, \quad \forall i, \tag{1}$$

which, can be written as the matrix equation,

$$\mathbf{l} = \mathbf{Ce}, \tag{2}$$

where $\mathbf{l} = [l_i]_{1\leq i\leq NK}$. If the channels are all mutually orthogonal, then $c_{ij} = 0$, $\forall\ i \neq j$. Since $c_{ii} = 0$, $\forall\ i$, the leakage, $l_i = 0$, $\forall\ i$. Since fragmentation results in non-orthogonal channels, $l_i \neq 0$, in general. The power leaked on the i^{th} channel can be obtained as l_i^2. The average power leaked on all the channels in the system, $\overline{P}_{\text{leaked}}$, can be written as

$$\overline{P}_{\text{leaked}} = \frac{1}{NK}\sum_{i=1}^{NK} l_i^2 = \frac{1}{NK}\mathbf{l}^H\mathbf{l} = \frac{1}{NK}\mathbf{e}^H\mathbf{C}^H\mathbf{Ce}, \tag{3}$$

where $(.)^H$ represents the Hermitian of a vector or a matrix.

Ideally, the malicious attackers[1] transmit so that the power, P_{tot}, is allocated over all the channels, such that the impact on each of the channels is highest. In order determine the impacts on all the channels, the attacker should have an exact knowledge of all the applications on all the channels in the system, which may not be possible in general. A more practical scenario is when the attacker tried to maximize the average power due to leakage, $\overline{P}_{\text{leaked}}$, which can be formulated as the following optimization problem

$$\max_{\mathbf{e}} \mathbf{e}^H \mathbf{C}^H \mathbf{C} \mathbf{e} = \max_{\mathbf{e}} \mathbf{e}^H \mathbf{A} \mathbf{e}, \tag{4}$$

(where $\mathbf{A} \stackrel{\triangle}{=} \mathbf{C}^H \mathbf{C}$), subject to the constraint,

$$\sum_{i=1}^{NK} P_i = \mathbf{e}^H \mathbf{e} \leq P_{\text{tot}}. \tag{5}$$

The matrix, $\mathbf{A}$, is a Hermitian matrix (i.e., $\mathbf{A}^H = \mathbf{A}$) and hence, has real eigen values [28]. Let $\mathbf{P}$ be the matrix whose columns are the eigen-vectors of $\mathbf{A}$. Since $\mathbf{A}$ is a Hermitian matrix, $\mathbf{P}$ can be chosen to be unitary [28] (i.e., $\mathbf{P}^H \mathbf{P} = \mathbf{P}\mathbf{P}^H$ =the identity matrix, $\mathbf{I}$). The vector, $\mathbf{e}$ can be written as [28]

$$\mathbf{e} = \mathbf{P}\mathbf{d}, \tag{6}$$

where $\mathbf{d} = [d_i]_{1 \leq i \leq NK}$ is another vector of length, NK. Let the set of eigen-values of $\mathbf{A}$ (called the spectrum of $\mathbf{A}$ [28]), $\sigma(\mathbf{A})$, be $\sigma(\mathbf{A}) = \{\lambda_1, \lambda_2, \cdots, \lambda_{NK}\}$ and without loss of generality, let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{NK}$. Such an ordering is possible since λ_i's are real.

It is then possible to formulate the optimization problem in (4) subject to (5), in terms of $\mathbf{d}$. Note that if $\mathbf{P}$ is unitary in (6), then $\mathbf{e}^H \mathbf{e} = \mathbf{d}^H \mathbf{d}$ [28], from which (5) can be written as

$$\mathbf{d}^H \mathbf{d} = \sum_{i=1}^{NK} d_i^2 \leq P_{\text{tot}}. \tag{7}$$

The optimization problem in (4) can then be re-written in terms of $\mathbf{d}$ as

$$\max_{\mathbf{d}} \mathbf{d}^H \mathbf{P}^H \mathbf{A} \mathbf{P} \mathbf{d} = \max_{\mathbf{d}} \mathbf{d}^H \mathbf{D} \mathbf{d}, \tag{8}$$

where $\mathbf{D}$ is the diagonal matrix, $\text{diag}(\lambda_1, \lambda_2, \cdots \lambda_n)$. Therefore, the optimization problem described in (8) subject to (7), is the optimization problem,

$$\max_{\mathbf{d}} \sum_{i=1}^{NK} U(\mathbf{d}) = \max_{\mathbf{d}} \sum_{i=1}^{NK} \lambda_i d_i^2 \tag{9}$$

subject to

$$\sum_{i=1}^{NK} d_i^2 \leq P_{\text{tot}}. \tag{10}$$

The following lemmas and theorem will be used to solve the optimization problem in (9) subject to (10), which, in turn, will be used to solve (4) subject to (5).

[1]Henceforth, throughout the paper, whenever we use the term, "malicious attackers," it may indicate a set of attackers, some transmitting on a single channel and some attackers transmitting on more than one channel. Alternatively, this may also represent a single attacker transmitting on all the channels.

Lemma 2.1: If $\lambda_k < 0$, $d_k = 0$ at the optimum point.

Proof: The statement uses the fact that the objective function in (9)is a weighted sum of positive quantities, with the weights being the eigen values, λ_i. Therefore, to maximize the weighted sum, the terms corresponding to negative weights must be zero. The detailed proof is provided in Appendix A. ■

Lemma 2.1 implies that positive d_i's should be allocated only corresponding to positive eigen values. The following lemma provides a constraint on the positive d_i's.

Lemma 2.2: Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$ and let $\lambda_i < 0$, $i > m$, $m \leq NK$. At the optimum point, $\sum_{i=1}^{m} d_i^2 = P_{\text{tot}}$, i.e., (10) is met with equality.

Proof: The proof uses the fact that the convex objective function in (9) subject to convex constraints in (10) is maximized when the constraints are met with equality. See Appendix B for the detailed proof. ■

From Lemmas 2.1 and 2.2, the following theorem which yields the optimum point, $\mathbf{d}^*$, can be obtained.

Theorem 2.1: Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$, $m \leq NK$ and $\lambda_i < 0$, $i > m$. The objective function in (9) subject to (10) is maximized for $\mathbf{d} = \mathbf{d}^* = [d_i^*]_{1 \leq i \leq NK}$ such that $d_1^* = \sqrt{P_{\text{tot}}}$ and $d_i^* = 0$, $i = 2, 3, \cdots, NK$.

Proof: The proof follows from the fact that the maximum point of convex the objective function in (9) subject to convex constraints, (10) occurs at an extreme point. The details are provided in Appendix C. ■

Since $\mathbf{d}^H \mathbf{d} = \mathbf{e}^H \mathbf{e}$, the malicious attackers transmit on all the channels such that (5) is met with equality. The optimal vector, $\mathbf{e}^*$ that solves (4) subject to (5) can be obtained from (6) with $\mathbf{d}$ replaced by $\mathbf{d}^*$. The following theorem characterizes $\mathbf{e}^*$.

Theorem 2.2: Let $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_m > 0$, $m \leq NK$. Let the eigen-vector of $\mathbf{A}$ corresponding to λ_1 be $\mathbf{x}_1 = [x_{i1}]_{1 \leq i \leq NK}$. Then $\mathbf{e}^* = \sqrt{P_{\text{tot}}} \mathbf{x}_1$ and the optimal power on the i^{th} channel, $P_i^* = P_{\text{tot}} |x_{i1}|^2$.

Proof: The proof, explained in detail in Appendix D, follows from the relation between the vectors, $\mathbf{d}$ and $\mathbf{e}$ given by (6). ■

It is noted that in general, x_{i1} can be non-zero, $\forall$ i and hence, the malicious attackers transmit non-zero powers on all the fragments (i.e., all malicious attackers may be actively transmitting) to create maximum leakage.

In the case of aggregation or bonding with no fragmentation, a similar scenario arises, which is explained as follows. Let the system contain N channels and let channels m and n be aggregated to result in $N-1$ channels in the system. Let m^* denote the new channel obtained by aggregating channels m and n. The channel, m^* need not be orthogonal to the other channels in the system and this, in turn can cause leakage into other channels. Similarly transmission on other channels can cause leakage into m^*. The analysis described in this section can then be used to determine the transmit power of the attacker on each channel.

Let $\tilde{\eta}$ be the white noise on all the channels in the absence of the leakage due to the transmission by the malicious attacker. Let the signal power on the i^{th} fragment be S_i. The signal-to-noise-ratio (SNR) on the i^{th} fragment, γ_i, is then given by $\gamma_i = \frac{S_i}{\tilde{\eta}}$. In the presence of leakage due to transmission

by a malicious attacker, the signal-to-interference-noise-ratio (SINR) on the i^{th} fragment, $\hat{\gamma}_i$, can be written as $\hat{\gamma}_i = \frac{S_i}{l_i^2+\eta}$, where $l_i = \sum_{j=1}^{NK} C_{ij}e_j^*$. Note that $\hat{\gamma}_i < \gamma_i$, thus resulting in a degraded signal quality. For a channel with bandwidth, B, This degradation can result in a degradation in the channel capacity by an amount, $B\log_2\left(\frac{1+\gamma_i}{1+\hat{\gamma}_i}\right)$.

Remark 1: It is noted that jamming a particular channel also causes loss of capacity. However, fragmentation causes a larger threat because a malicious attacker can transmit on channel j to cause a loss of capacity on channel i. This kind of an attack is a result of fragmentation and aggregation because of loss of orthogonality between the fragments. Hence, the service disruption caused by the malicious attacker as a consequence of fragmentation and aggregation, is a cognitive service disruption where the attackers intelligently transmit powers on the channels to disrupt service on the other channels.

Remark 2: Note that when the malicious attackers decide to launch a MAXIMP attack, they transmit at P_{tot} according to Theorem 2.2. The malicious attackers have transmit at maximum power to create maximum impact. In other words, they cannot transmit at a lesser power.

III. MINPOW Attack

Consider an advanced LTE or HSPA+ network with $\hat{N}$ orthogonal carriers. Some of these carriers can be aggregated or bonded to result in $N < \hat{N}$ bonded/aggregated carriers[2]. Henceforth, throughout this section, "channel" refers to one of the N aggregated/bonded carriers in the system, unless explicitly mentioned otherwise. The malicious attackers wish to exploit the loss of orthogonality due to channel bonding/ aggregation to cause service disruption. In LTE and HSPA+ networks, it may not be practically feasible to transmit at maximum power all the time because of transmit power regulations by the base stations. Further, here, the attackers target specific users to whom they wish to create service disruption, because only one user uses a channel at a time. The malicious attackers know the application of the targeted user and can launch an attack to disrupt the service of the targeted user, depending on the applications incident on the user, by using MINimum POWer.

In order to perform the analysis to launch the MINPOW attack, we consider the covariance matrix, $\mathbf{C}$, the field strength vector, $\mathbf{e}$ and the power vector, $\mathbf{p}$, as defined in Section II. In the MINPOW attack, the attackers utilize minimum power so that $\overline{P}_{\text{leaked}}$ is large enough (greater than a threshold, $\epsilon^* = N\epsilon$), to cause significant service disruption. This can be formulated as the following optimization problem

$$\min_{\mathbf{e}} \sum_{i=1}^{N} P_i = \min_{\mathbf{e}} \mathbf{e}^H\mathbf{e}, \tag{11}$$

subject to the constraints,

$$\mathbf{e}^H\mathbf{C}^H\mathbf{C}\mathbf{e} = \mathbf{e}^H\mathbf{A}\mathbf{e} \geq \epsilon, \tag{12}$$

[2]It is noted that we do not analyze channel fragmentation in this case because the LTE and HSPA+ define aggregation and bonding but not channel fragmentation.

It is noted that the MINPOW attack problem in (11) subject to (12) is **not** the dual of the MAXIMP problem, (4) subject to (5). Hence, the results discussed in Section II do not trivially extend for this attack. As in Section II, let $\mathbf{P}$ be the unitary matrix whose columns are the eigen-vectors of $\mathbf{A}$ and let $\sigma(\mathbf{A}) = \{\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N\}$ be the spectrum of $\mathbf{A}$.

It is then possible to formulate the optimization problem in (11) subject to (12), in terms of $\mathbf{d}$ as

$$\min_{\mathbf{d}} \mathbf{d}^H\mathbf{d} = \min_{\mathbf{d}} \sum_{i=1}^{N} d_i^2, \tag{13}$$

subject to the constraint (12), which, becomes

$$\mathbf{d}^H\mathbf{P}^H\mathbf{A}\mathbf{P}\mathbf{d} = \mathbf{d}^H\mathbf{D}\mathbf{d} = \sum_{i=1}^{N} \lambda_i d_i^2 \geq \epsilon. \tag{14}$$

Applying Lemma 2.1 to the optimization problem in (13) subject to the constraint, (14), we can also state the following lemma and theorem.

Lemma 3.1: Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$ and let $\lambda_i < 0$, $i > m$, $m \leq N$. At the optimum point, $\sum_{i=1}^{m} \lambda_i d_i^2 = \epsilon$, i.e., (14) is met with equality.

Proof: The proof follows from the fact that a convex optimization problem with convex constraints attains its optimum point when the constraints are met with equality. A formal proof is provided in Appendix E. ■

Theorem 3.1: Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$, $m \leq N$ and $\lambda_i < 0$, $i > m$. The objective function in (13) subject to (14) is minimized for $\mathbf{d} = \mathbf{d}^* = [d_i^*]_{1\leq i\leq N}$ such that $d_1^* = \sqrt{\frac{\epsilon}{\lambda_1}}$ and $d_i^* = 0$, $i = 2, 3, \cdots, N$.

Proof: The proof, explained in Appendix F is similar to the one for Theorem 2.1. ■

Since $\mathbf{e} = \mathbf{P}\mathbf{d}$, $\mathbf{e}^*$=$\sqrt{\frac{\epsilon}{\lambda_1}}\mathbf{x}_1$, where $\mathbf{x}_1 = [x_{i1}]_{1\leq i\leq N}$ is the eigen vector corresponding to λ_1. Also, since $\mathbf{d}^H\mathbf{d} = \mathbf{e}^H\mathbf{e}$, the minimum power transmitted by the attacker is $\frac{\epsilon}{\lambda_1}$. Since the total power that the attacker can transmit over all the channels is P_{tot}, it follows that the attack is feasible if and only if $\epsilon \leq P_{\text{tot}}\lambda_1$. As mentioned in Section II, in general, x_{i1} can be non-zero, $\forall\ i$ and hence, the attackers may be required to transmit non-zero powers on all the channels.

The reduced signal-to-interference-noise ratio (SINR) at each receiving user in the system can be measured because the power transmitted by the attackers cause additional interference to the user. The reduced SINR results in larger bit error rate (BER), which represents the percentage loss in the data throughput. The BER depends on the SINR and the modulation used. We consider quadrature phase shift keying (QPSK) 16 point quadrature amplitude modulation (16-QAM) and 64 point quadrature amplitude modulation (64-QAM) in our analysis as specified in the LTE [17] and HSPA [18] standards.

Note that the exact modulation scheme depends on the location of the mobile users in the cell. Users near the base station typically deploy 64-QAM, users towards the periphery of the cell use QPSK and uses that are near the base station nor near the periphery deploy 16-QAM [17], [18]. In order to measure the loss in throughput due to the MINPOW attack, it is

essential to perform simulation experiments where in, users are generated to occupy random locations in a multi-cell system and the interference due to the attack is measured, taking into account, radio propagation characteristics. The impact of the MINPOW attack can be quantitatively measured by computing the average impact over multiple simulation experiments. The details of the simulation experiment including the considered radio propagation characteristics, is explained in Section V-B.

Remark 3: It is observed that due to the practical constraints of malicious attackers being unable to target individual users in 802.22 WRANs and being unable to transmit at maximum power in LTE and HSPA+ networks because of policy enforcement in the standards, they can only launch MAXIMP attack in DSA based 802.22 WRANs and only launch MINPOW in LTE and HSPA+ networks.

IV. Detection of the Attacks

It was observed from Sections II and III that the attackers either transmit at maximum possible power, P_{tot}, to launch the MAXIMP attack in IEEE 802.22 WRANs or with minimum power, $P_{\min} = \frac{\epsilon}{\lambda_1}$, to launch the MINPOW attack. The network can then detect this attack due to collusion between the attackers by one of two mechanisms- (i) determining the correct channels to bond or aggregate or fragment or (ii) based on the degradation in throughput they suffer, based on which, they can estimate the received signal strength. Determining the correct channels to bond or aggregate or fragment is equivalent to determining the correlation matrix, $\mathbf{C}$, that has the smallest value of the largest eigen vector, λ_1, which is very complex because, in a system with NK fragments, the number of correlation matrices that should be considered is of the order of 2^{NK}. Therefore, we discuss detection of the attack based on the received signal strength, i.e., option (ii) mentioned above.

The good nodes can transmit at any power, $P_g \in [0, P_{\text{tot}}]$. In the absence of power control the good nodes transmit at P_{tot} on all the channels and in the presence of power control, the nodes transmit at an average power, P_{ave}. The attackers either transmit at P_{tot} (while launching MAXIMP attacks in DSA based 802.22 WRANs) or $P_{\min} = \frac{\epsilon}{\lambda_1}$ (while launching MINPOW attack in LTE and HSPA+ networks)[3] The signal undergoes distance attenuation, log-normal shadowing and Rayleigh fading [29]. Conditioned on the distance and Rayleigh fading terms, the received power at any good node can be modeled as a log-normal random variable, when represented in Watts and a Gaussian random variable, when represented in decibels (dB). Let x (in dB) be the received power at any good node. When the attack takes place $x \sim \mathcal{N}(\mu_a, \sigma_a^2)$ and when no attack takes place, $x \sim \mathcal{N}(\mu_g, \sigma_g^2)$. The good node then uses this received power to decide if an attack took place or if it just obtained the received signal as a consequence of interference.

[3]Note that it is not optimal for the the attackers to transmit at any other power because the transmit powers of the attackers are obtained by solving the optimization problems (4) and (11) subject to the constraints, (5) and (12), respectively. The exact solutions are provided by Theorems 2.2 and 3.1.

First a likelihood ratio, $\Lambda(x)$ is computed as

$$\Lambda(x) = \frac{\exp\left(-\frac{(x-\mu_a)^2}{2\sigma_a^2}\right)}{\exp\left(-\frac{(x-\mu_g)^2}{2\sigma_g^2}\right)}. \tag{15}$$

Then, the good nodes decide if they detected an attack or not, by using the decision rule

$$\Lambda(x) \underset{\text{noattack}}{\overset{\text{attack}}{\gtrless}} \Lambda_0, \tag{16}$$

where the optimal value of the threshold, Λ_0, is $\Lambda_0 = 1$ [30]. When $\sigma_g^2 = \sigma_a^2 = \sigma_n^2$ (as will be shown later from (19)), the optimal decision in (16) for $\Lambda_0 = 1$ becomes

$$x \underset{\text{noattack}}{\overset{\text{attack}}{\gtrless}} \frac{\mu_g + \mu_a}{2}. \tag{17}$$

The probability of detecting this attack, p_{detect}, is then evaluated as

$$p_{\text{detect}} = \Pr\left\{x > \frac{\mu_g + \mu_a}{2} | \text{ attack is launched}\right\} = 1 - Q\left(\frac{\mu_a - \mu_g}{2\sigma_n}\right). \tag{18}$$

The parameters, μ_a, σ_a, μ_g and σ_g are obtained as follows. As mentioned earlier, each good user receives a signal from $\overline{M}$ other users in the system (both good users as well as attackers). Note that to know the value of $\overline{M}$ it requires the knowledge of the number of other good users and the number of jammers. While the number of good users can be obtained from the system level parameters, the number of jammers is estimated by localization techniques presented in [31]-[35]. Let the power received from the i^{th} user be $y_i = 10^{-\frac{\xi_i}{10}}$, where $\xi_i \sim \mathcal{N}(\tilde{\mu}, \sigma^2)$ when a good user transmits and $\xi_i \sim \mathcal{N}(\hat{\mu}, \sigma^2)$ when attackers transmit. The total received power, x, will then be $y = \sum_{i=1}^{\overline{N}} y_i$, which is the sum of several log-normally distributed random variables, which, according to Fenton's method [36] can be approximated as a log-normal random variable, i.e., $y = 10^{-\frac{x}{10}}$, where $x \sim \mathcal{N}(\mu_g, \sigma_g^2)$ when good users transmit and $x \sim \mathcal{N}(\mu_a, \sigma_a^2)$ when attackers launch the attack.

In [37], Anand *et al* applied Fenton's approximation to determine the parameters of a log-normally distributed random variable. Applying the analysis in [37] here, μ_g, σ_g, μ_a and σ_a are obtained as

$$\sigma_g^2 = \sigma_a^2 \triangleq \sigma_n^2 = \frac{1}{a^2}\ln\left(1 + \frac{e^{a^2\sigma^2} - 1}{\overline{M}}\right), \tag{19}$$

where $a = \frac{\ln 10}{10}$,

$$\mu_g = \tilde{\mu} - \frac{1}{a}\ln \overline{M} + \frac{a}{2}\left(\sigma_n^2 - \sigma^2\right) \tag{20}$$

and

$$\mu_a = \hat{\mu} - \frac{1}{a}\ln \overline{M} + \frac{a}{2}\left(\sigma_n^2 - \sigma^2\right). \tag{21}$$

In (20) and (21),

$$\tilde{\mu} = 10\log_{10} P_{\text{ave}} - 40\log_{10}\left(\frac{2R}{3}\right) + 20\log_{10} R_f, \tag{22}$$

where $P_{\rm ave} = P_{\rm tot}$ in the absence of power control and in the presence of power control, $P_{\rm ave} = \overline{P}$, the average transmit power due to power control[4], R is the cell radius and R_f is the mean Rayleigh fade. Like wise,

$$\hat{\mu} = 10\log_{10} P_{\rm attack} - 40\log_{10}\left(\frac{2R}{3}\right) + 20\log_{10} R_f, \quad (23)$$

where $P_{\rm attack} = P_{\rm tot}$ for the MAXIMP attack and $P_{\rm attack} = \frac{\epsilon}{\lambda_1}$ for the MINPOW attack. From (18), (19)-(23), the probability of detecting the attack, $p_{\rm detect}$, can be written as

$$p_{\rm detect} = 1 - Q\left(\frac{1}{2\sigma_n} 10\log_{10}\left(\frac{P_{\rm attack}}{P_{\rm ave}}\right)\right). \quad (24)$$

It is noted that in general, $p_{\rm detect} \neq 1$, indicating that it is not possible to *always* detect the attack. Infact, from (24), the probability of detection is larger when $P_{\rm attack}$ and $P_{\rm ave}$ are significantly different from each other and when $P_{ave} \approx P_{\rm attack}$, then $p_{\rm detect} \to 0$. Therefore, the success of the detection mechanism depends on the difference between the average transmit power of the good users, $P_{\rm ave}$ and the transmit power of the attackers, $P_{\rm attack}$.

Remark 4: It is observed that the receivers are not required to know who the good users and who the malicious attackers are, in order to perform the detection. The receivers only use the received signal, x, and compare it with a threshold specified in (17). The threshold depends only on *the value* of the transmit powers of the attackers and good nodes and not on which node is good and which node is an attacker.

The detection probability can be enhanced further by a centralized co-operation between the good users. The good users make an individual decision on whether the received signal was a transmission from another good user or whether it was due to an attack, using the decision rule in (16). Then, they all convey their individual decisions to a centralized controller which could be the base station. Once the base station receives all the individual decisions from all the nodes, it aggregates all these individual decisions to arrive at a refined co-operative decision to detect the attack. In [38], Jin and the co-authors of this paper had developed a centralized protocol to improve the spectrum decision to detect a denial of service (DoS) attack in DSA networks. We adopt a similar protocol here to refine the individual detection mechanism. The co-operative detection mechanism is described in Algorithm 1.

Remark 5: Upon detection of the attack, the system can choose more efficient way of bonding channels, i.e., choose to bond channels, so that largest singular value of the covariance matrix, $\mathbf{C}$ (i.e., the largest eigen value of the matrix, $\mathbf{A} = \mathbf{C}^H\mathbf{C}$), is minimum. However, this problem is very complex and heuristics need to be developed to bond/aggregate or fragment channels appropriately.

Remark 6: It is observed that the MAXIMP attack (discussed in Section II) and the MINPOW attack (discussed in Section III) are not the only attacks that can be launched by the malicious attackers. The attackers can also choose to launch an attack wherein, the probability of detecting the attack is very small. Such an attack may be sub-optimal, i.e., may not create maximum impact or may not use minimum transmit power, but the attack can be camouflaged effectively. Discussion on such attacks is a separate topic and out of scope of this paper. The detection mechanisms discussed in this paper may not be as effective for those attacks, and alternative detection mechanisms need to be designed.

[4]Note that the average value, $\overline{P}$ depends on the exact power control mechanism deployed. Since it is out of the scope of this paper to discuss specific power control mechanisms, we consider users the average case where users transmit at powers uniformly distributed in $[0, P_{\rm tot}]$ and hence $\overline{P} = \frac{1}{2}P_{\rm tot}$.

Algorithm 1 Co-operative decision mechanism where in all users co-operate in a centralized manner to detect the attack

1) The $\overline{M}$ nodes convey their individual decisions on detecting the attack, to the base station.
2) The base station aggregates all the individual results and counts the number of nodes, $\tilde{M}$, who conclude that the received signal was due to an attack according to the decision rule in (16).
3) Let $0 < \overline{L} < \overline{U} < 1$. The refined co-operative decision performed by the base station is
   a) If $\tilde{M} > \overline{UM}$, then the base station concludes that an attack has been launched.
   b) If $\tilde{M} < \overline{LM}$, then the base station concludes that there is no attack.
   c) If $\overline{LM} < \tilde{M} < \overline{UM}$, then the base station concludes that there is an attack, with a probability $p_{\rm attack} = \frac{\tilde{M} - \overline{LM}}{\overline{UM} - \overline{LM}}$ and concludes that there is no attack with probability, $1 - p_{\rm attack}$.

V. Results and Discussion

We discuss the numerical results of the MAXIMP attack in Section V-A and those of the MINPOW attack in Section V-B. As mentioned in Section I, we consider the IEEE 802.22 WRAN for the MAXIMP attack and the LTE and HSPA+ networks for the MINPOW attack. Section V-C presents the results of the detection mechanism discussed in Section IV.

A. MAXIMP Attack

We consider two systems, one with $N = 3$ orthogonal channels (like the IEEE 802.22), each with bandwidth, 20 MHz, fragmented into $K = 3$ fragments, each with bandwidth, 6.66 MHz, thus resulting in $NK = 9$ fragments in the system. We also study a system with $N = 13$ orthogonal channels each fragmented into $K = 3$ fragments, to result in $NK = 39$ fragments in the system. We first consider a fixed value of $P_{\rm tot}$ and compute the optimal transmit powers on all the channels in the system with $NK = 9$ fragments. We then vary the total power that can be transmitted by the malicious attackers, P_{tot}, and study the average loss in the capacity due to leakage. The optimal transmit power of the malicious attacker hence, the leakage on each channel, is obtained using the analysis described in Section II. The covariance matrix, $\mathbf{C}$ is generated using the standard inner product of the carrier frequencies [39].

Table I presents the transmit powers on all the fragments for 10 malicious attackers with $P_{\rm tot} = 10$ Watts, in a system

TABLE I

TRANSMIT POWERS FOR THE MALICIOUS ATTACKER LAUNCHING MAXIMP ATTACK IN AN IEEE 802.22 WRAN, WITH $P_{\text{tot}} = 10$ WATTS, ON EACH FRAGMENT IN A SYSTEM WITH $N = 3$ ORTHOGONAL CHANNELS EACH FRAGMENTED INTO $K = 3$ FRAGMENTS.

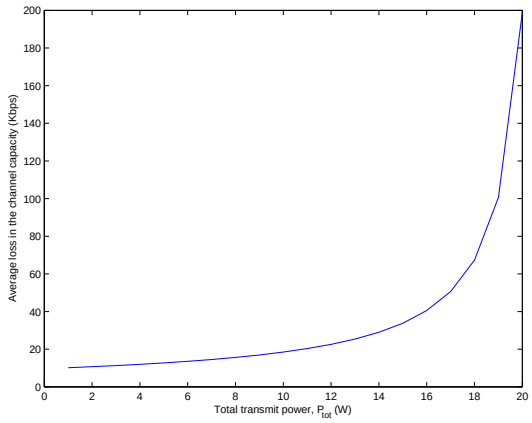
Fragment	Power (P_i)
1	235 mW
2	945 mW
3	133.6 mW
4	1.536 Watts
5	430.8 mW
6	673.7 mW
7	2.374 Watts
8	3.397 Watts
9	274.7 mW

with $N = 3$ orthogonal channels, each fragmented into $K = 3$ fragments, thus resulting in $NK = 9$ fragments. It is observed that the transmit powers on all the fragments are non-zero, as argued in Section II. It is observed from Table I, that a small transmit power by a malicious user on any fragment (e.g., 133 mW in fragment 3) can also result in maximum leakage on that fragment when combined with a larger transmit power from another malicious user on another fragment (e.g., 3.4 Watts in fragment 8). This reinforces the argument presented in Section I about cognitive service disruption resulting as a consequence of fragmentation. The average loss in the capacity was found to be 20 Kbps.

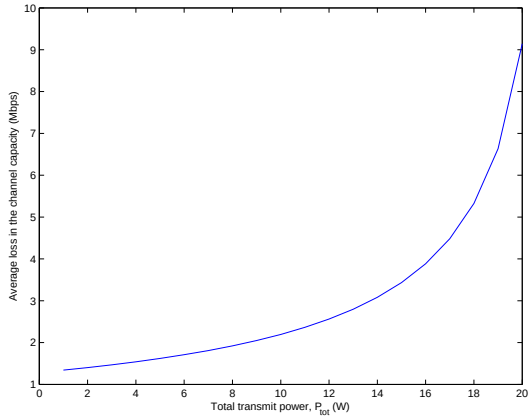
We vary the total transmit power, P_{tot}, and determine the average loss in capacity. This is equivalent to varying the number of malicious users. Fig. 2(a) presents the average loss in the capacity in a system with $N = 3$ orthogonal channels each fragments into $K = 3$ fragments, thus resulting in $NK = 9$ fragments. It is observed that the loss in capacity is negligible for low values of the total transmit power, P_{tot}, where as, for large values of P_{tot}, the loss is significant. In other words, fewer malicious users cause negligible service disruption but a larger number of users can cause significant service disruption. The loss in capacity can be as large as 200 Kbps, which, for a system supporting 1-2 Mbps, is a loss of about 16%. The average loss is larger in the system with $N = 13$ orthogonal channels fragmented into $K = 3$ fragments (which typically supports 54 Mbps [6]), resulting in $NK = 39$ fragments, as observed from Fig. 2(b). Here, loss of the order of up to 9 Mbps is observed. In a system supporting 54 Mbps traffic, this corresponds to a loss in capacity by 11%. The larger loss in capacity is caused due to that fact that there are larger number of fragments and hence, correlations between multiple pairs of fragments. This enables the attacker to transmit in more fragments and cause service disruption.

B. MINPOW Attack

To obtain the numerical results for the MINPOW attack, we consider a 19-macro cell LTE and HSPA system. About 100000 simulation experiments were conducted on UBUNTU Linux platform. In each experiment, users are generated with locations uniformly distributed in the area of each cell so that there are 10 near users (using 64-QAM), 10 far users (using QPSK) and 10 users using 16-QAM in each cell. We take $P_{\text{tot}} = 10$ Watts and ϵ is chosen so that $\epsilon << P_{\text{tot}}\lambda_1$.



(a) $N = 3$ orthogonal channels



(b) $N = 13$ orthogonal channels

Fig. 2. Average loss in the capacity due to the MAXIMP attack in an IEEE 802.22 WRAN network with N orthogonal channels each fragmented into $K = 3$ fragments.

Channels in the LTE system are aggregated according to the specification in [8] [40], where in, among five channels (centered at 460 MHz, 700 MHz, 803 MHz, 2.6 GHz and 3.75 GHz) [7] the 700 MHz and the 2.6 GHz channels are aggregated. Channels in the HSPA+ system (1 GHz, 1.5 GHz and 2 GHz bands) are aggregated in the HSPA+ system as specified in [15]. Channel gains to the users from the base stations or E-Node B's and the attacker are generated using the Jake's model [29]. The attackers generate powers on different channels according to the Theorem 3.1 discussed in Section III. For each simulation trial, the random channel gain generated according to Jake's model is used in conjunction with the correlation between the aggregated carriers, to compute the additional interference suffered by each user due to malicious attackers. The additional interference is used to compute the signal-to-interference noise ratio (SINR), which, in turn, is used to compute the bit error rate (BER) for QPSK, 16-QAM and 64-QAM users. The BER also gives the percentage loss in throughput. by each node. The loss in throughput is then

averaged out over all the 100000 simulation experiments.

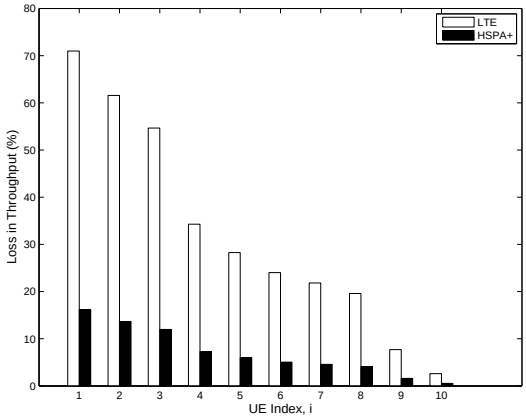


Fig. 3. Average loss in the throughput due to the MINPOW attack, for far users deploying QPSK in a system with 19 cells. Users are indexed such that whenever $i < j$, user i receives less signal strength from the E Node B than user j.

Figs. 3-5 depict the average loss in throughput in the LTE and HSPA+ networks for the *far users* deploying QPSK (Fig. 3), users that are *neither near nor far*, deploying 16-QAM (Fig. 4) and *near users* deploying 64-QAM (Fig. 5). It is observed from Fig. 3, that the attack discussed in this paper can cause significant loss in throughput for the far users. Particularly, in LTE systems, this loss could be as high as 70%. The impact is much lesser on the high data rate users who are either near the E node B's (using 64-QAM) or between the E Node B's and the periphery of the cells (using 16-QAM). This is because, these users being nearer to the E Node Bs are farther from the attacker and perceive lesser impact in terms of percentage loss. However, a loss in throughput of 3-4% (for 64-QAM LTE users) corresponds to a loss in throughput of about 1.7 Mbps when two 20 Mbps channels are aggregated. Therefore the theoretical throughput of 42 Mbps mentioned in [8] does not really yield 42 Mbps but yields only 40 Mbps, which is a significant loss. This loss is more significant for HSPA+ networks as it corresponds to a loss of 4-6 Mbps, thus resulting only in 34 Mbps as against the theoretical rate of 40 Mbps.

Also, Figs. 3 and 4 suggest that the impact on the throughput due to channel bonding in LTE Advanced networks is more significant (about 70% reduction) than that in HSPA+ networks (about 15%) for the far users and the users that are neither near nor at the periphery of the cells. From Fig. 5, near users in HSPA+ networks suffer larger degradation in throughput (12%) due to channel bonding than those in advanced LTE networks (3-4%). This is because, the correlation between channels in HSPA+ networks is larger than that in LTE networks. However, the absolute throughput of far users in HSPA+ networks is less than that in LTE networks. Therefore, although the throughput decreases for far users both in LTE as well as in HSPA networks, the percentage in the degradation in LTE networks is more prominent. For near users though, the absolute throughput is large both in LTE as well as in HSPA networks and hence, the degradation in throughput due to the large correlation between channels in HSPA networks is more evident.

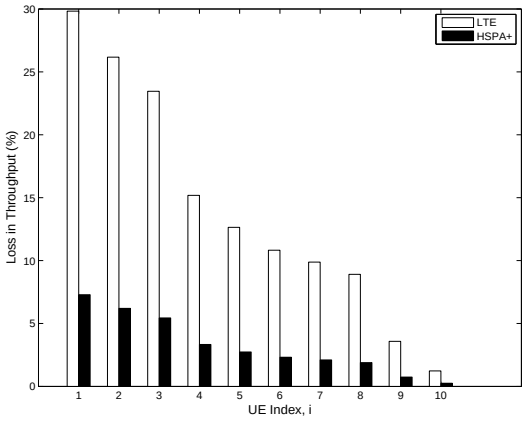


Fig. 4. Average loss in the throughput due to the MINPOW attack, for users neither near the E Node B or at the periphery, deploying 16-QAM, in a system with 19 cells. Users are indexed such that whenever $i < j$, user i receives less signal strength from the E Node B than user j.

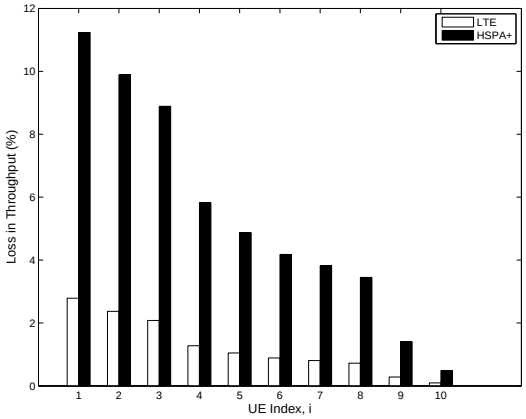
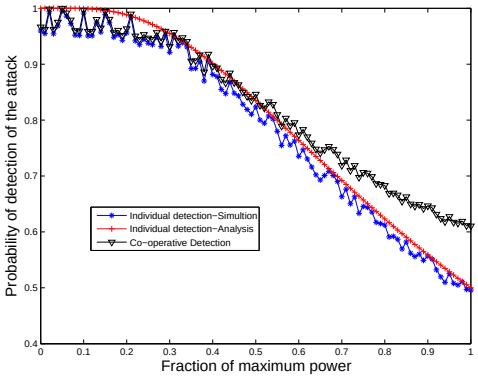


Fig. 5. Average loss in the throughput due to the MINPOW attack, for near users deploying QPSK in a system with 19 cells. Users are indexed such that whenever $i < j$, user i receives less signal strength from the E Node B than user j.

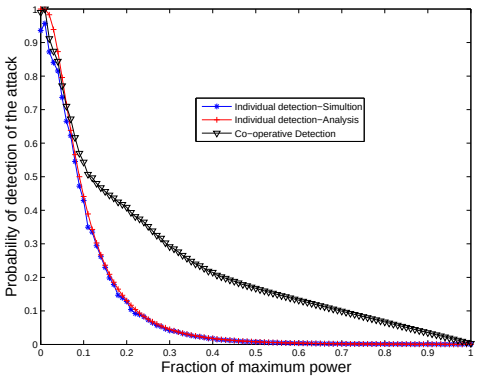
C. Detection of the attack

Finally, we also study the probability of detection of the attacks in Fig. 6. We first study the probability of detection of the MAXIMP attack. We study cases of power control with different values of P_{ave}. Fig 6(a) depicts the probability of detection of the MAXIMP attack. As observed in Section II, the attackers transmit at P_{tot}, while the good users can deploy power control with different values of the average power, P_{ave}. It is noted that as $P_{\text{ave}} \to P_{\text{tot}}$, the probability of detection, $p_{\text{detect}} \to 0$. This is intuitively true because when $P_{\text{ave}} \to P_{\text{tot}}$, the good users also transmit at P_{tot}, like the attackers rendering failure of detection of the attack. In other words, the MAXIMP attack can be detected by effective power control. While reducing P_{ave} results in better detection of the attack, one cannot reduce P_{ave} indefinitely because too low transmit powers may result in poor SINR, i.e., poor performance.

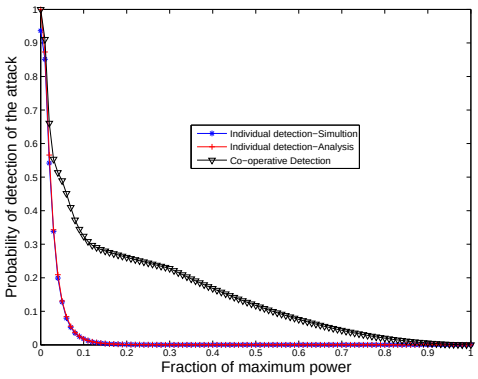
We then study the probability of detection of the MINPOW attack. We consider an LTE network and an HSPA



(a) MAXIMP



(b) MINPOW LTE



(c) MINPOW HSPA

Fig. 6. Probability of successful detection of the attack for the MAXIMP attack (Fig. 6(a)), for the MINPOW attack in an LTE system (Fig. 6(b)) and MINPOW attack in an HSPA system (Fig. 6(c)).

network. Figs. 6(b) and 6(c) show the probability of successful detection of the MINPOW attack in the LTE and HSPA system, respectively. It is observed that the probability of detecting the attack is much lower than that in the MAXIMP attack This is because, in the MINPOW attack, the attackers transmit at minimum power to launch an effective attack. When the average power of the good users increases, then the good users are more likely to believe that the degradation in the signal quality is due to interference than due to the attack. The consequence is that the probability of detecting the attack decreases. However, the probability of detection can be enhanced by using the assistance of the centralized controller (e.g., base station) to make a co-operative decision, as described in Section IV. For the computations here, we choose $\overline{U} = 0.75$ and $\overline{L} = 0.25$. Note that while deploying the centralized detection, the malicious attackers also convey their decision to the centralized controller. It was shown in [38] that the attackers maximize their likelihood for launching the attack successfully, when they *ALWAYS* convey their own decision as "no attack." Hence, here also, in our experiments, we assume that the decision conveyed by the attackers is that the service degradation is always due to interference and not due to the attack.

Another observation that can be made is that the attack is more likely to be detected in an LTE network than in an HSPA network. This is because, the value of λ_1 is larger in the HSPA system, indicating that the attackers transmit at lesser power. As P_{ave} increases, it becomes much larger than the optimal transmit power of the attackers. Therefore, the degradation suffered due to interference is more than that due to the attack. Then, users can hardly detect the attack. As observed in the results in Section V-B, for near users, the degradation in throughput in HSPA system is more and for far users the degradation in the LTE system is more. Since the average distance from the eNodeB is $2R/3$ where R is the cell radius, which corresponds to the location of far users, the degradation in throughput in the LTE system is larger and hence, the attack is more likely to be detected in the LTE system.

VI. Conclusion

We identified a unique security vulnerability due to channel fragmentation, aggregation and bonding, that could lead to service disruption in IEEE 802.22 WRAN, 3GPP advanced LTE and HSPA+ networks. We presented analyses for two types of attacks- the MAXIMP attack in IEEE 802.22 WRAN where malicious users try to create maximum impact and the MINPOW attack where in malicious users transmit at minimum powers to create sufficient impact. Some key inferences drawn include

- Bonding or aggregating two channels of specified capacities does not yield a channel with the sum of the capacities (the total capacity obtained is less than the sum of its parts).
- The MAXIMP attack can result in loss of capacity of up to 16%.

- Far users or low data rate users perceive larger impact in loss of throughput due to MINPOW attack, than near high data rate users.
- The impact of MINPOW attack on far users is larger in advanced LTE networks than in HSPA+ networks while near users in HSPA+ networks suffer larger impact than those in advanced LTE networks.
- MAXIMP attacks can be detected by deploying power control.
- MINPOW attacks can be more easily detected in LTE systems than in HSPA systems. However, MINPOW attacks are not so easy to detect as the MAXIMP attack.

Other mechanisms to mitigate such attacks includes determination of an optimal subset of bonded/ fragmented/ aggregated channels and the corresponding matrix, $\mathbf{A} = \mathbf{C}^H\mathbf{C}$, whose maximum eigen value, λ_1, is minimum. This is a min-max optimization of a discrete set of possibilities. The number of matrices that need to be considered are $\sum_{K=1}^{N} \binom{N}{K}$, which is of the order of 2^N, for N channels and hence, is NP-hard in general. We are currently investigating some heuristics to determine the right channels to bond or aggregate or fragment. Other possible attacks and detection mechanisms to mitigate those attacks, are topics for investigation in future.

APPENDIX A
PROOF OF LEMMA 2.1

Let $\tilde{\mathbf{d}} = \left[\tilde{d}_i\right]_{1\le i\le NK}$ be a feasible solution such that $\tilde{d}_k > 0$. Consider another solution $\hat{\mathbf{d}} = \left[\hat{d}_i\right]_{1\le i\le NK}$, where $\hat{d}_k = 0$ and $\hat{d}_j = \tilde{d}_j$, $\forall\ j \neq k$. Since $\tilde{\mathbf{d}}$ is a feasible point, $\sum_i \tilde{d}_i^2 \le P_{\text{tot}}$, i.e., $\sum_i \hat{d}_i^2 \le P_{\text{tot}}$. Therefore, $\hat{\mathbf{d}}$ is also a feasible point. The proof is complete if it can be shown that $U(\tilde{\mathbf{d}}) < U(\hat{\mathbf{d}})$.

$$\begin{aligned} U(\tilde{\mathbf{d}}) &= \sum_{i=1}^{NK} \lambda_i \tilde{d}_i^2 \\ &= \sum_{\substack{i=1\\ i\neq k}}^{NK} \lambda_i \tilde{d}_i^2 + \lambda_k \tilde{d}_k^2 \\ &= \sum_{\substack{i=1\\ i\neq k}}^{NK} \lambda_i \hat{d}_i^2 + \lambda_k \tilde{d}_k^2 \\ &< \sum_{\substack{i=1\\ i\neq k}}^{NK} \lambda_i \hat{d}_i^2 \text{ since } \lambda_k < 0 \\ &= U(\hat{\mathbf{d}}). \end{aligned}$$

APPENDIX B
PROOF OF LEMMA 2.2

From Lemma 2.1, $d_i = 0, \forall i > m$. Consider a feasible point $\tilde{\mathbf{d}} = \left[\tilde{d}_i\right]_{1\le i\le m}$ such that $\sum_{i=1}^{m} \tilde{d}_i^2 = \tilde{P} < P_{\text{tot}}$. Let $\Delta \triangleq P_{\text{tot}} - \tilde{P}$. It is noted that $\Delta > 0$. Consider $\hat{\mathbf{d}} = \left[\hat{d}_i\right]_{1\le i\le m}$, such that $\hat{d}_m = \tilde{d}_m + \sqrt{\Delta}$ and $\hat{d}_i = \tilde{d}_i$, $i = 1, 2, \cdots, m-1, m+1, \cdots NK$. Therefore,

$$\begin{aligned} \sum_{i=1}^{NK} \hat{d}_i^2 &= \sum_{i=1}^{m} \hat{d}_i^2 \\ &= \sum_{i=1}^{m-1} \tilde{d}_i^2 + \hat{d}_m^2 \\ &= \sum_{i=1}^{m-1} \tilde{d}_i^2 + \tilde{d}_m^2 + \Delta \\ &= \tilde{P} + \Delta = P_{\text{tot}}, \end{aligned}$$

i.e., $\hat{\mathbf{d}}$ is also a feasible point with $\sum_{i=1}^{m} \hat{d}_i = P_{\text{tot}}$.

$$\begin{aligned} U(\hat{\mathbf{d}}) &= \sum_{i=1}^{m} \lambda_i \hat{d}_i^2 \\ &= \sum_{i=1}^{m-1} \lambda_i \tilde{d}_i^2 + \lambda_i \hat{d}_m^2 \\ &= \sum_{i=1}^{m-1} \lambda_i \tilde{d}_i^2 + \lambda_i \tilde{d}_m^2 + \Delta \\ &= U(\tilde{\mathbf{d}}) + \Delta \\ &> U(\tilde{\mathbf{d}}) \text{ since } \Delta > 0. \end{aligned}$$

APPENDIX C
PROOF OF THEOREM 2.1

From Lemma 2.1, $d_i^* = 0$, $\forall\ i > m$. Let $\tilde{\mathbf{d}} = \left[\tilde{d}_i\right]_{1\le i\le m}$ such that $\tilde{d}_i > 0$, $1 \le i \le m$ and $\sum_{i=1}^{m} \tilde{d}_i = P_{\text{tot}}$, according to Lemma 2.2. Therefore,

$$U(\tilde{\mathbf{d}}) = \sum_{i=1}^{m} \lambda_i \tilde{d}_i^2 \le \sum_{i=1}^{m} \lambda_1 \tilde{d}_i^2 = \lambda_1 P_{\text{tot}} = \lambda_1 \left(d_1^*\right)^2 = U(\mathbf{d}^*).$$

APPENDIX D
PROOF OF THEOREM 2.2

From (6)

$$\mathbf{e}^* = \mathbf{P}\mathbf{d}^*.$$

Since $d_1^* = \sqrt{P_{\text{tot}}}$ and $d_i^* = 0$, $2 \le i \le NK$ from Theorem 2.1,

$$\mathbf{e}^* = d_1^*\mathbf{x}_1 = \sqrt{P_{\text{tot}}}\mathbf{x}_1.$$

Since $P_i^* = |E_i^*|^2$,

$$P_i^* = P_{\text{tot}} \left|x_{i1}\right|^2, \tag{25}$$

resulting in $P_i^* \ge 0$, $\forall i$ and $\sum_{i=1}^{NK} P_i = P_{\text{tot}}$, i.e., feasible transmit powers on all the fragments.

APPENDIX E
PROOF OF LEMMA 3.1

From Lemma 2.1, $d_i = 0, \forall i > m$. Consider a feasible point $\tilde{\mathbf{d}} = \left[\tilde{d}_i\right]_{1\le i\le m}$ such that $\sum_{i=1}^{m} \lambda_i \tilde{d}_i^2 = \tilde{\epsilon} > \epsilon$. Let $\Delta \triangleq \tilde{\epsilon} - \epsilon$. It is noted that $\Delta > 0$. Consider $\hat{\mathbf{d}} = \left[\hat{d}_i\right]_{1\le i\le m}$, such that $\hat{d}_m = \sqrt{\left|\tilde{d}_m^2 - \frac{\Delta}{\lambda_m}\right|}$ and $\hat{d}_i = \tilde{d}_i$, $i = 1, 2, \cdots, m-1, m+1, \cdots N$. Therefore,

$$\sum_{i=1}^{m} \lambda_i \hat{d}_i^2 = \sum_{i=1}^{m} \lambda_i \tilde{d}_i^2 - \Delta = \tilde{\epsilon} - \Delta = \epsilon,$$

i.e., $\hat{\mathbf{d}}$ is also feasible and

$$\sum_{i=1}^{N} \hat{d}_i^2 = \sum_{i=1}^{m-1} \tilde{d}_i^2 + \tilde{d}_m^2 - \frac{\Delta}{\lambda_m} < \sum_{i=1}^{N} \tilde{d}_i^2.$$

APPENDIX F
PROOF OF THEOREM 3.1

From Lemma 3.1 and constraint (14),

$$\begin{aligned} \textstyle\sum_{i=1}^{N} \lambda_i d_i^2 &= \epsilon, \\ \text{i.e., } \textstyle\sum_{i=1}^{m} \lambda_i d_i^2 &= \epsilon, \\ \text{i.e., } \lambda_1 \textstyle\sum_{i=1}^{m} d_i^2 &\ge \epsilon, \\ \text{i.e., } \textstyle\sum_{i=1}^{m} d_i^2 &\ge \frac{\epsilon}{\lambda_1}, \end{aligned}$$

with equality if and only if $d_1^* = \sqrt{\frac{\epsilon}{\lambda_1}}$ and $d_i^* = 0$, $i = 2, 3, \cdots, N$.

ACKNOWLEDGMENT

This research was partially funded by NSF CCF # 0916180, partially funded by NSF CNS # 0917008 and partially funded by NSF CNS # 1346600.

REFERENCES

[1] S. Anand, K. Hong, S. Sengupta, and R. Chandramouli, "Is channel fragmentation/bonding in IEEE 802.22 networks secure?" *Proc., IEEE Intl. Conf. on Commun. (ICC'2011)*, Jun. 2011.

[2] S. Anand, K. Hong, S. Sengupta, R. Chandramouli, and K. P. Subbalakshmi, "Security vulnerability due to channel aggregation/bonding in LTE and HSPA+ networks," *Proc., IEEE Global Commun. Conf (GLOBECOM'2011)*, Dec. 2011.

[3] M. Buddhikot, P. Kolodzy, S. Miller, K. Ryan, and J. Evans, "DIMSUMnet: New directions in wireless networking using coordinated dynamic spectrum access," *IEEE WoWMoM'2005*, Oct. 2005.

[4] M. Wyglinski, M. Nekovee, and Y. T. Hou, *Cognitive Radio Communications and Networks: Principles and Practice*. Elsevier Inc., 2010.

[5] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "Ieee 802.22: The first worldwide wireless standard based on cognitive radios," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2005*, pp. 328–337, Nov. 2005.

[6] "IEEE draft standard for information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Part 22.1: Standard to enhance harmful interference protection for low power licensed devices operating in the TV broadcast bands," Feb. 2009.

[7] [Online]. Available: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/4g-lte-advanced-carrier-channel-aggregation.php

[8] [Online]. Available: http://urgentcomm.com/networks_and_systems/news/lte-non-contiguous-spectrum-20110330/

[9] S. Sengupta, S. Brahma, M. Chatterjee, and N. S. Shankar, "Enhancements to cognitive radio based IEEE 802.22 air interface," *Proc. IEEE Intl. Conf. on Commun. (ICC'2007)*, pp. 5155–5160, Jun. 2007.

[10] H. Song and X. Lin, "A novel DSA driven MAC protocol for cognitive radio networks," *Wireless Sensor Networks*, vol. 61, no. 2, pp. 112–121, Feb. 2009.

[11] P. Bahl, R. Chandra, T. Moscibroda, R. Murthy, and M. Welsh, "White space networking withWi-Fi like connectivity," *Proc., SIGCOMM'2009*, Aug. 2009.

[12] S. Deb, V. Srinivasan, and R. Maheshwari, "Dynamic spectrum access in DTV white spaces: Design rules, architecture and algorithms," *Proc., ACM Intl. Conf. on Mobile Computing and Networking (ICMC('2009)*, Sep. 2009.

[13] E. Coffman, P. Robert, F. Simatos, S. Tarumi, and G. Zussman, "Channel fragmentation in dynamic spectrum access systems: A theoretical study," *ACM SIGMETRICS Perf. Eval. review*, vol. 38, no. 1, pp. 333–344, Jun. 2010.

[14] J. Geier, *Designing and Deploying 802.11n Wireless Networks*. Cisco Press, 2007.

[15] [Online]. Available: http://www.fiercebroadbandwireless.com/story/t-mobile-rolls-out-dual-carrier-hspa-put-it-par-verizons-lte/2011-03-24

[16] [Online]. Available: http://www.fiercebroadbandwireless.com/special-reports/carrier-aggregation-how-att-will-use-qualcomms-mediaflo-spectrum-double-lte?utm_medium=rss&utm_source=rss

[17] "3GPP TS 36.211: Evolved universal terrestrial radio access (EUTRA); Physical channels and modulation," Dec. 2010.

[18] "3GPP TS 25.317: High speed packet access (HSPA); Requirements on user equipments (UE's) support for release independent frequency band combination," Dec. 2010.

[19] [Online]. Available: http://www.networkingwolrd.com/newsletters/2004/0119wireless2.html

[20] L. Deek, E. Garcia-Villegas, E. Belding, S. Lee, and K. Almeroth, "The impact of channel bonding on IEEE 802.11 network management," *Proc., ACM CoNEXT'2011*, Dec. 2011.

[21] V. Angelakis, S. Papadakis, V. A. Siris, and A. Traganitis, "Adjacent channel interference in 802.11a is harmful: Test bed verification of a simple quantification model."

[22] L. Yang, B. Y. Zhao, and H. Zheng, "The space between us: Setting and maintaining boundaries in wireless spectrum access," *Proc., IEEE MOBICOM2010*, Sep. 2010.

[23] S. Sengupta, K. Hong, R. Chandramouli, and K. P. Subbalakshmi, "Spiderradio: A cognitive radio network with commodity hardware and open source software," *IEEE Commun. Mag.*, vol. 49, no. 3, pp. 101–109, Mar. 2011.

[24] T. Basar, "A Gaussian test channel with an intelligent jammer," *IEEE Trans. on Info. Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[25] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, "Multi-channel jamming attacks using cognitive radios," *Proc. IEEE Intl. Conf. on Computer Commun. and Networking (ICCCN'2007)*, Aug. 2007.

[26] S. Anand, S. Sengupta, and R. Chandramouli, "An attack-defense game theoretic analysis of multi-band wireless covert timing networks," *Proc. IEEE Intl. Conf. on Computer Commun. (INFOCOM'2010)*, Mar. 2010.

[27] I. F. Akyildiz, D. M. Guttierrez-Estevez, and E. C. Reyes, "The evolution of 4G cellular systems: LTE-advanced," *Elsevier Phy. Commun.*, vol. 3, no. 4, pp. 217–244, Dec. 2010.

[28] C. D. Meyer, *Matrix Theory and Applied Linear Algebra*. SIAM, 1972.

[29] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall Inc., New Jersey, 1996.

[30] M. D. Srinath and P. K. Rajasekaran, *An introduction to statistical signal processing with applications*. John Wiley and Sons, 1978.

[31] T. Cheng, P. Li, and S. Zhu, "An algorithm for jammer localization in wireless networks," *Proc., IEEE Intl. Conf. on Advaned Info. Networking and Applications (AINA'2012)*, Mar. 2012.

[32] Y. S. Kim, F. Mokaya, E. Chen, and P. Tague, "All your jammers belong to us - Localization of wireless sensors under jamming attack," *Proc., IEEE Intl. Conf. on Commun. (ICC'2012)*, Jun. 2012.

[33] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proc., MobiHoc' 2005*, Jun. 2005.

[34] Z. Liu, H. Liu, W. Xu, and Y. Chen, "An error minimizing framework for localizing jammers in wireless networks," *IEEE Trans. on Parallel and Distributed Computing*, Feb. 2013.

[35] A. Boustani, N. R. Alamatsaz, M. Jadliwala, and V. Namboodiri, "LocJam: A novel jamming-based approach to secure localization in wireless networks," *IEEE Consumer Commun. and Networking Conf. (CCNC'2014)*, Jan. 2014.

[36] L. F. Fenton, "The sum of log-normal probability distributions in scatter transmission systems," *IRE Trans. on Commun. Systems*, vol. CS-8, no. 3, pp. 57–67, Mar. 1960.

[37] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," *Proc., IEEE Symposium for New Frontiers in Dynamic Spectrum Access Networks (DySPAN'2008)*, Oct. 2008.

[38] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Robust spectrum decision protocol resilient to primary user emulation attacks in dynamic spectrum access networks," *Proc., IEEE GLOBECOM 2010*, Dec. 2010.

[39] Y. Shmaliy, *Continuous-time Signals (Signals and Communication Technology*. Springer, 2006.

[40] [Online]. Available: http://www.eetimes.com/design/microwave-rf-design/4212869/Introducing-LTE-Advanced?pageNumber=1